Build Security In Home

What is Build Security In?

Build Security In is a collaborative effort that provides practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development.

Introduction to Software Security[1]

Call for Authors and Reviewers

Submit an article for publication on BSI or volunteer to review new articles. See the Call for Authors and Reviewers[2] for details.

Community Collaboration

To access other software assurance materials or to join the collaboration efforts of a related working group, visit the DHS Software Assurance Program's Community Resources and Information Clearinghouse[3].

Sponsor and Contributors

Build Security In is a Software Assurance[4] strategic initiative of the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security. Peer-reviewed material submitted by many authors is presented for public use. Staff of Carnegie Mellon University's Software Engineering Institute contribute and review articles and maintain the site. Many other organizations have contributed articles to BSI (see Contributing Authors[5]), and submission of articles[6] is welcome.

Improve Security and Software Assurance: Tackle the CWE Top 25 – The Most Dangerous Programming Errors

The Top 25 CWEs represent the most significant exploitable software constructs that have made software so vulnerable. Addressing these will go a long way in securing software, both in development and in operation. Read more and see the list of Top 25 CWE Programming Errors[7] on the Software Assurance Community Resources and Information Clearinghouse website.

Consistent with this list is the Top 10 for 2010 released by the Open Web Application Security Project (OWASP). OWASP's report captures the top ten risks associated with the use of web applications in an enterprise. Download the report, which contains examples and details that explain these risks to software developers, managers, and anyone interested in the future of web security, for free here[8].

What's New

Calls for papers have been posted for the Second IEEE International Conference on Information Privacy, Security, Risk, and Trust (PASSAT[9]), the 1st International Workshop on Measurability of Security in Software Architectures (MeSSa),[10] and the Software Assurance Minitrack of the 44th Hawaii International Conference on System Sciences (HICSS-44).[11]

A new article, Improving Software Assurance[12], has been added.

A new article, Supply-Chain Risk Management: Incorporating Security into Software Development[13], has been added to the Acquisition [14]content area.

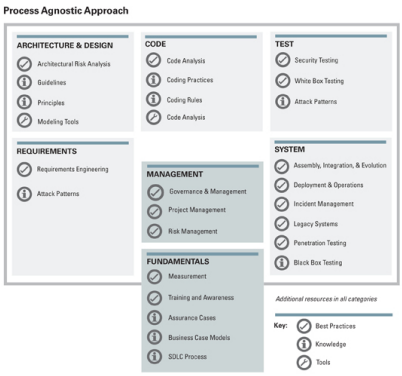
Information about the June Software Assurance Working Group Sessions[15] (June 21-23, 2010), the Software Assurance Forum[16] (September 27-October 1, 2010), and the December Software Assurance Working Group Sessions[17] (December 14-16, 2010) has been posted.

BSI Updates

A newsletter describing additions to and significant revisions of BSI content is emailed periodically to subscribers. Follow the instructions[18] to subscribe or unsubscribe.

Process Agnostic Approach

BSI articles are grouped in a process agnostic view[19]. The content areas are classified in the following sections: Requirements, Architecture & Design, Code, Test, System, Management, and Fundamentals. Click on the thumbnail graphic at right to access navigation by process category.



20

Ten Most Recently Modified Articles

Name	Content Areas	Version Creation Time	Abstract
Improving Software Assurance	knowledge/assurance	4/7/10 12:48:15 PM	Software assurance objectives include reducing the likelihood of vulnerabilities such as those on a Top 25 Common Weakness Enumeration[21] (CWE) list and increasing confidence that the system behaves as expected. Practitioners

should understand where to look, what to look for, and how to demonstrate improvement.

For practitioners who want to delve deeper into software assurance, the BSI website provides a wealth of information to aid in tying security into all development activities. For example, the BSI website[22] includes a number of papers[23] that were presented at the Making the Business Case for Software Assurance Workshop[24] in September 2008. Today, more than 25 large-scale software security initiatives are underway in organizations as diverse as multi-national banks, independent software vendors, the U.S. Air Force, and embedded systems manufacturers. The Software Assurance Forum for Excellence in Code (SAFECode), an industry-leading non-profit organization that focuses on the advancement of effective software assurance methods, published a report on secure software development [Simpson 2008]. In 2009, the first version of The Building Security In Maturity Model (BSIMM) was published [McGraw 2009]. BSIMM was created from a survey of nine organizations with active software security initiatives the authors considered to be the most advanced. The nine organizations were drawn

			from three verticals: four financial services firms, three independent software vendors, and two technology firms. Those companies among the nine who agreed to be identified include Adobe, The Depository Trust & Clearing Corporation (DTCC), EMC, Google, Microsoft, QUALCOMM, and Wells Fargo.
Supply-Chain Risk Management: Incorporating Security into Software Development	best-practices/acquisition	3/25/10 3:03:03 PM	**Supply-Chain Risk Management: Incorporating Security into Software Development**[25] As outsourcing and expanded use of commercial off-the-shelf (COTS) products increase, supply-chain risk becomes a growing concern for software acquisitions. Supply-chain risks for hardware procurement include manufacturing and delivery disruptions,[26] and the substitution of counterfeit or substandard components. Software supply-chain risks include third-party tampering with a product during development or delivery and, more likely, a compromise of the software assurance through the introduction of software defects. This paper describes practices that address such defects and mechanisms for introducing these practices into the acquisition life cycle. The practices improve the likelihood of predictable behavior

			by systematically analyzing data flows to identify assumptions and using knowledge of attack patterns and vulnerabilities to analyze behavior under conditions that an attacker might create.
Requirements Elicitation Case Studies Using IBIS, JAD, and ARM	best-practices/ requirements	3/1/10 3:42:26 PM	This article describes a tradeoff analysis that can be done to select a suitable requirements elicitation method and the results of trying three methods in some case studies. It is a companion to the requirements elicitation introduction[27].
Application Firewalls and Proxies - Introduction and Concept of Operations	best-practices/assembly	3/1/10 3:32:21 PM	Practices that could significantly improve application security by integrating knowledge about an application's specific security needs into elements of the IT security infrastructure are often overlooked. This document describes one of the many potential topic areas involving the integration of business applications into a supporting IT security infrastructure. Application firewalls attempt to use application-specific knowledge to improve the perimeter defense that the security infrastructure provides.
Deployment and Operations References	best-practices/ deployment	1/6/10 2:52:42 PM	Content area bibliography.
Assembly, Integration, and Evolution Overview	best-practices/assembly	1/6/10 2:51:41 PM	The objective of the Assembly, Integration & Evolution content area is to raise awareness about the essential technical, business, and individual user issues that must be addressed during

			assembly, integration, and evolution to achieve and maintain a high degree of system-wide assurance of security and survivability.
Governance and Management References	best-practices/governance	12/1/09 3:03:32 PM	Content area bibliography.
Security Is Not Just a Technical Issue	best-practices/governance	11/30/09 12:47:57 PM	Updates to this material are, in part, either adapted or excerpted from *Software Security Engineering: A Guide for Project Managers* [Allen 2008[28]]. This overview defines the scope of governance concern as it applies to security. It describes some of the top-level considerations and characteristics to use as indicators of a security conscious culture and whether an effective program is in place.
Maturity of Practice	best-practices/governance	11/30/09 11:41:13 AM	Updates to this material are, in part, either adapted or excerpted from Software Security Engineering: A Guide for Project Managers [Allen 2008][29]. This article identifies several indicators that organizations are addressing security as a governance and management concern, at the enterprise level. It summarizes how some organizations, trade associations, and market sectors are proceeding. Many of the references and links in this article provide more detailed implementation guidance.
How Much Security Is Enough?	best-practices/governance	11/30/09 11:16:54 AM	Updates to this material are, in part, either adapted or excerpted

			from Software Security Engineering: A Guide for Project Managers [Allen 2008][30]. This article provides guidelines for answering this question, including strategy questions to ask, organizational and market characteristics to take into account, and means for determining adequate security based on risk. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken.